

# New MDS Euclidean and Hermitian self-dual codes over finite fields

Hongxi Tong<sup>1</sup> Xiaoqing Wang<sup>2</sup>

Department of Mathematics, Shanghai University, Shanghai 200444.<sup>1 2</sup>  
(email: tonghx@shu.edu.cn<sup>1</sup> 2625453656@qq.com<sup>2</sup>)

**Abstract:** In this paper, we construct MDS Euclidean self-dual codes which are extended cyclic duadic codes. And we obtain many new MDS Euclidean self-dual codes. We also construct MDS Hermitian self-dual codes from generalized Reed-Solomon codes and constacyclic codes. And we give some results on Hermitian self-dual codes, which are the extended cyclic duadic codes.

**Keywords:** MDS Euclidean self-dual codes, MDS Hermitian self-dual codes, constacyclic codes, cyclic duadic codes, generalized Reed-Solomon codes.

## 1 Introduction

Let  $\mathbb{F}_q$  denote a finite field with  $q$  elements. An  $[n, k, d]$  linear code  $C$  over  $\mathbb{F}_q$  is a  $k$ -dimensional subspace of  $\mathbb{F}_q^n$ . These parameters  $n$ ,  $k$  and  $d$  satisfy  $d \leq n - k + 1$ . If  $d = n - k + 1$ ,  $C$  is called a maximum distance separable (MDS) code. MDS codes are of practical and theoretical importance. For examples, MDS codes are related to geometric objects called  $n$ -arcs.

The Euclidean dual code  $C^\perp$  of  $C$  is defined as

$$C^\perp := \left\{ x \in \mathbb{F}_q^n : \sum_{i=1}^n x_i y_i = 0, \forall y \in C \right\}.$$

If  $q = r^2$ , the Hermitian dual code  $C^{\perp H}$  of  $C$  is defined as

$$C^{\perp H} := \left\{ x \in \mathbb{F}_{r^2}^n : \sum_{i=1}^n x_i y_i^r = 0, \forall y \in C \right\}.$$

If  $C$  satisfies  $C = C^\perp$  or  $C = C^{\perp H}$ ,  $C$  is called Euclidean self-dual or Hermitian self-dual, respectively. There are many papers discussing Euclidean self-dual codes or Hermitian self-dual codes.<sup>[2][12]</sup> If  $C$  is MDS and Euclidean self-dual or Hermitian self-dual,  $C$  is called an MDS Euclidean self-dual code or an MDS Hermitian self-dual code, respectively. In recent years, study of MDS self-dual codes has attracted a lot of attention.<sup>[1][2][3][4][5][6][8][9]</sup> One of these problems in this topic is to determine existence of MDS self-dual codes. When  $2|q$ , Grassl and Gulliver completely solve the existence of MDS Euclidean self-dual codes in [4]. In [5], Guenda obtain some new MDS Euclidean self-dual codes and MDS Hermitian self-dual codes. In [8], Jin and Xing obtain some new MDS Euclidean self-dual codes from generalized Reed-Solomon codes.

In this paper, we obtain some new Euclidean self-dual codes by studying the solution of an equation in  $\mathbb{F}_q$ . And we generalize Jin and Xing's results to MDS Hermitian self-dual codes. We also construct MDS Hermitian self-dual codes from constacyclic codes. We discuss MDS Hermitian self-dual codes obtained from extended cyclic duadic codes. We give some corrections of the result on MDS Hermitian self-dual codes obtained from extended cyclic duadic codes in [5].

## 2 MDS Euclidean Self-Dual Codes

A cyclic code  $C$  of length  $n$  over  $\mathbb{F}_q$  can be considered as an ideal,  $\langle g(x) \rangle$ , of the ring  $R = \frac{\mathbb{F}_q[x]}{x^n - 1}$ , where  $g(x) | x^n - 1$  and  $(n, q) = 1$ . The set  $T = \{0 \leq i \leq n - 1 | g(\alpha^i) = 0\}$  is called the defining set of  $C$ , where  $\text{ord} \alpha = n$ .

Let  $S_1$  and  $S_2$  be unions of cyclotomic classes modulo  $n$ , such that  $S_1 \cap S_2 = \emptyset$  and  $S_1 \cup S_2 = \mathbb{Z}_n \setminus \{0\}$  and  $aS_i \pmod{n} = S_{i+1 \pmod{2}}$ . Then the triple  $\mu_a$ ,  $S_1$  and  $S_2$  is called a splitting modulo  $n$ . Odd-like codes  $D_1$  and  $D_2$  are cyclic codes over  $\mathbb{F}_q$  with defining sets  $S_1$  and  $S_2$ , respectively.  $D_1$  and  $D_2$  can be denoted by  $\mu_a(D_i) = D_{i+1 \pmod{2}}$ . Even-like duadic codes  $C_1$  and  $C_2$  are cyclic codes over  $\mathbb{F}_q$  with defining sets  $\{0\} \cup S_1$  and  $\{0\} \cup S_2$ , respectively. Obviously,  $\mu_a(C_i) = C_{i+1 \pmod{2}}$ . A duadic code of length  $n$  over  $\mathbb{F}_q$  exists if and only if  $q$  is a quadratic residue modulo  $n$ .<sup>[11]</sup>

Let  $n|q-1$  and  $n$  be an odd integer.  $D_1$  is a cyclic code with defining set  $T = \{1, 2, \dots, \frac{n-1}{2}\}$ . Then  $D_1$  is an  $[n, \frac{n+1}{2}, \frac{n+1}{2}]$  MDS code. Its dual  $C_1 = D_1^\perp$  is also cyclic with defining set  $T \cup \{0\}$ . There are a pair of odd-like duadic codes  $D_1 = C_1^\perp$  and  $D_2 = C_2^\perp$  and a pair of even-like duadic codes  $C_2 = \mu_{-1}(C_1)$ .

**Lemma 1**<sup>[5]</sup> Let  $n|q-1$  and  $n$  be an odd integer. There exists a pair of MDS codes  $D_1$  and  $D_2$  with parameters  $[n, \frac{n+1}{2}, \frac{n+1}{2}]$ , and  $\mu_{-1}(D_i) = D_{i+1 \pmod{2}}$ .

**Lemma 2**<sup>[7]</sup> Let  $D_1$  and  $D_2$  be a pair of odd-like duadic codes of length  $n$  over  $\mathbb{F}_q$ ,  $\mu_{-1}(D_i) = D_{i+1 \pmod{2}}$ . Assume that

$$1 + \gamma^2 n = 0 \quad (*)$$

has a solution in  $\mathbb{F}_q$ . Let  $\tilde{D}_i = \{\tilde{c} | c \in D_i\}$  for  $1 \leq i \leq 2$  and  $\tilde{c} = (c_0, c_1, \dots, c_{n-1}, c_\infty)$  with  $c_\infty = -\gamma \sum_{i=0}^{n-1} c_i$ . Then  $\tilde{D}_1$  and  $\tilde{D}_2$  are Euclidean self-dual codes.

In [7], the solution of  $(*)$  is discussed when  $n$  is an odd prime. In [5], the solution of  $(*)$  is discussed when  $n$  is an odd prime power. Next, we discuss the solution of  $(*)$  for any odd integer  $n$  with  $n|q-1$ .

**Definition 1 (Legendre Symbol)**<sup>[10]</sup> Let  $p$  be a prime and  $a$  be an integer.

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \pmod{p}, \\ 1, & \text{if } a (\not\equiv 0) \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is not a quadratic residue modulo } p. \end{cases}$$

**Proposition 1**<sup>[10]</sup>

$$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_s}{p}\right),$$

where  $a = p_1 \cdots p_s$ .

**Definition 2 (Jacobi Symbol)**<sup>[10]</sup> Let  $m$  and  $n(\neq 0)$  be two integers.

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_h}\right),$$

where  $n = p_1 \cdots p_h$ .

We cannot obtain  $m(\neq 0)$  is a quadratic residue modulo  $n$  from  $\left(\frac{m}{n}\right) = 1$ . But we have the next proposition.

**Proposition 2** Let  $m(\neq 0)$  and  $n$  be two integers and  $(m, n) = 1$ . If  $m$  is a quadratic residue modulo  $n$ , then

$$\left(\frac{m}{n}\right) = 1.$$

If

$$\left(\frac{m}{n}\right) = -1,$$

then  $m$  is not a quadratic residue modulo  $n$ .

Proof Obviously.

**Lemma 3 (Law of Quadratic Reciprocity)**<sup>[10]</sup> Let  $p$  and  $r$  be odd primes,  $(p, r) = 1$ .

$$\left(\frac{p}{r}\right) \left(\frac{r}{p}\right) = (-1)^{\frac{r-1}{2} \cdot \frac{p-1}{2}}.$$

**Corollary 1** Let  $p$  and  $r$  be odd primes.

(1) When  $p \equiv 1(\text{mod } 4)$  or  $r \equiv 1(\text{mod } 4)$ ,

$$\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right).$$

(2) When  $p \equiv r \equiv 3(\text{mod } 4)$ ,

$$\left(\frac{p}{r}\right) = -\left(\frac{r}{p}\right).$$

**Theorem 1** Let  $q = r^t$  and  $r$  be an odd prime. Let  $n|q-1$  and  $n$  be an odd integer. And

$$n = p_1^{e_1} \cdots p_s^{e_s} p_{s+1}^{e_{s+1}} \cdots p_h^{e_h},$$

where

$$p_1 \equiv \cdots \equiv p_s \equiv 3(\text{mod } 4), \quad p_{s+1} \equiv \cdots \equiv p_h \equiv 1(\text{mod } 4).$$

(1) When  $q \equiv 1(\text{mod } 4)$ , there is a solution to  $(*)$  in  $\mathbb{F}_q$ .

(2) Let  $q \equiv 3(\text{mod } 4)$ . If  $\sum_{i=1}^s e_i$  is an odd integer, there is a solution to (\*) in  $\mathbb{F}_q$ .

Proof (1)  $q \equiv 1(\text{mod } 4)$ .

(1.1)  $r \equiv 3(\text{mod } 4)$ . So we have that  $t$  is even. Then every quadratic equation with coefficients in  $\mathbb{F}_r$ , such as Eq. (\*), has a solution in  $\mathbb{F}_{r^2} \subseteq \mathbb{F}_q$ .

(1.2)  $r \equiv 1(\text{mod } 4)$  and  $2|t$ . The proof is similar as (1.1).

(1.3)  $r \equiv 1(\text{mod } 4)$  and  $2 \nmid t$ .

$$1 = \left(\frac{q}{n}\right) = \left(\frac{r}{n}\right) = \left(\frac{r}{p_1}\right)^{e_1} \cdots \left(\frac{r}{p_h}\right)^{e_h} = \left(\frac{p_1}{r}\right)^{e_1} \cdots \left(\frac{p_h}{r}\right)^{e_h} = \left(\frac{n}{r}\right).$$

So  $n$  is a quadratic residue modulo  $r$ . And  $-1$  is a quadratic residue modulo  $r$ . So there is a solution to (\*) in  $\mathbb{F}_q$ .

(2)  $q \equiv 3(\text{mod } 4)$ . Then  $r \equiv 3(\text{mod } 4)$  and  $t$  is odd.

$$\begin{aligned} 1 &= \left(\frac{q}{n}\right) = \left(\frac{r}{n}\right) = \left(\frac{r}{p_1}\right)^{e_1} \cdots \left(\frac{r}{p_s}\right)^{e_s} \left(\frac{r}{p_{s+1}}\right)^{e_{s+1}} \cdots \left(\frac{r}{p_h}\right)^{e_h} \\ &= (-1)^{e_1} \left(\frac{p_1}{r}\right)^{e_1} \cdots (-1)^{e_s} \left(\frac{p_s}{r}\right)^{e_s} \left(\frac{p_{s+1}}{r}\right)^{e_{s+1}} \cdots \left(\frac{p_h}{r}\right)^{e_h} \\ &= (-1)^{\sum_{i=1}^s e_i} \left(\frac{p_1}{r}\right)^{e_1} \cdots \left(\frac{p_s}{r}\right)^{e_s} \left(\frac{p_{s+1}}{r}\right)^{e_{s+1}} \cdots \left(\frac{p_h}{r}\right)^{e_h} = (-1)^{\sum_{i=1}^s e_i} \left(\frac{n}{r}\right). \end{aligned}$$

If  $\sum_{i=1}^s e_i$  is odd,  $n$  is not a quadratic residue modulo  $r$ . And  $-1$  is not a quadratic residue modulo  $r$ . So  $-n$  is a quadratic residue modulo  $r$ . There is a solution to (\*) in  $\mathbb{F}_q$ .

**Remark** In fact,  $n|q-1$ , and  $n$  is an odd integer and  $q \equiv 3(\text{mod } 4)$ . We can easily prove that there is a solution to (\*) in  $\mathbb{F}_q$  if and only if  $\sum_{i=1}^s e_i$  is an odd integer.

Let  $n|q-1$ ,  $q \equiv 1(\text{mod } n)$ .  $q$  is a quadratic residue modulo  $n$ .  $y^2 \equiv q(\text{mod } n)$ . Let  $q = r^t$  and  $q \equiv 3(\text{mod } 4)$ , where  $r$  is a prime. Then  $r \equiv 3(\text{mod } 4)$  and  $t$  is odd. Eq. (\*) has solutions in  $\mathbb{F}_q$  if and only if Eq. (\*) has solutions in  $\mathbb{F}_r$ . And  $r$  is a quadratic residue modulo  $n$ .  $(yr^{-\frac{t-1}{2}})^2 \equiv r(\text{mod } n)$ . Let  $p$  be an odd prime divisor of  $n$ .  $r$  is a quadratic residue modulo  $p$ . Then  $\left(\frac{r}{p}\right) = 1$ . By Law of Quadratic Reciprocity,  $p|n$ ,

$$\left(\frac{p}{r}\right) = \begin{cases} 1, & p \equiv 1(\text{mod } 4) \\ -1, & p \equiv 3(\text{mod } 4) \end{cases}.$$

The Legendre symbol

$$\begin{aligned} \left(\frac{-n}{r}\right) &= \left(\frac{-1}{r}\right) \left(\frac{p_1}{r}\right)^{e_1} \cdots \left(\frac{p_s}{r}\right)^{e_s} \left(\frac{p_{s+1}}{r}\right)^{e_{s+1}} \cdots \left(\frac{p_h}{r}\right)^{e_h} \\ &= (-1)^{1+\sum_{i=1}^s e_i} = \begin{cases} 1, & \sum_{i=1}^s e_i \text{ is odd} \\ -1, & \sum_{i=1}^s e_i \text{ is even} \end{cases}, \end{aligned}$$

where  $n = p_1^{e_1} \cdots p_s^{e_s} p_{s+1}^{e_{s+1}} \cdots p_h^{e_h}$ ,  $p_1 \equiv \cdots \equiv p_s \equiv 3(\text{mod } 4)$  and  $p_{s+1} \equiv \cdots \equiv p_h \equiv 1(\text{mod } 4)$ .

**Theorem 2** Let  $q = r^t$  be a prime power,  $n|q-1$  and  $n$  be an odd integer. Then there exists a pair  $D_1, D_2$  of MDS odd-like duadic codes of length  $n$  and  $\mu_{-1}(D_i) = D_{i+1(\text{mod } 2)}$ , where even-like duadic codes are MDS self-orthogonal, and  $T_1 = \{1, \dots, \frac{n-1}{2}\}$ . Furthermore,

- (1) If  $q = 2^t$ , then  $\tilde{D}_i$  are  $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$  MDS Euclidean self-dual codes.
- (2) If  $q \equiv 1(\text{mod } 4)$ , then  $\tilde{D}_i$  are  $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$  MDS Euclidean self-dual codes.
- (3) If  $q \equiv 3(\text{mod } 4)$  and  $\sum_{i=1}^s e_i$  is an odd integer, then  $\tilde{D}_i$  are  $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$  MDS Euclidean self-dual codes, where  $n = p_1^{e_1} \cdots p_s^{e_s} p_{s+1}^{e_{s+1}} \cdots p_t^{e_h}$  and  $p_1 \equiv \cdots \equiv p_s \equiv 3(\text{mod } 4)$ ,  $p_{s+1} \equiv \cdots \equiv p_h \equiv 1(\text{mod } 4)$ .

**Proof** Obviously,  $D_i$  are  $[n, \frac{n+1}{2}, \frac{n+1}{2}]$  MDS odd-like duadic codes. If there is a solution to (\*), we want to prove  $\tilde{D}_i$  are  $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$  MDS Euclidean self-dual codes, and we only need to prove that

$$c \in D_i \text{ and } wt(c) = \frac{n+1}{2}, \text{ then } wt(\tilde{c}) = \frac{n+1}{2} + 1.$$

This is equivalent to prove that  $c_\infty \neq 0$ . It can be proved similarly by which proved in [5].

When  $q = 2^t$ , there is a solution to (\*) in  $\mathbb{F}_{2^t}$ ,  $\tilde{D}_i$  are  $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$  MDS Euclidean self-dual codes by Lemma 2.

We can obtain (2) and (3) from Theorem 1 and Lemma 2. Theorem 2 is proved.

We list some new MDS Euclidean self-dual codes in the next table.

n	q
4	$2^2, 7$
6	$2^4, 3^4$
8	$2^3, 3^6$
10	$2^6, 5^6$
12	$3^5$
14	$2^{12}, 3^6$
16	$31, 31^2, 31^3$
18	$3^{16}$
20	$5^9$
22	$5^6$
24	$3^{11}$
26	$7^4$
28	$7^9$
30	$59$
156	$5^4$

### 3 MDS Hermitian Self-Dual Codes

Let  $n \leq q^2$ . We choose  $n$  distinct elements  $\{\alpha_1, \dots, \alpha_n\}$  from  $\mathbb{F}_{q^2}$  and  $n$  nonzero elements  $\{v_1, \dots, v_n\}$  from  $\mathbb{F}_{q^2}$ . The generalized Reed-Solomon code

$$GRS_k(\alpha, v) := \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_{q^2}[x], \deg f(x) \leq k-1\}$$

is a  $q^2$ -ary  $[n, k, n-k+1]$  MDS code, where  $\alpha = (\alpha_1, \dots, \alpha_n)$  and  $v = (v_1, \dots, v_n)$ .

**Theorem 3** Let  $n \leq q$  and  $2|n$ . Let  $\{\alpha_1, \dots, \alpha_n\}$  be  $n$  distinct elements from  $\mathbb{F}_q(\subseteq \mathbb{F}_{q^2})$  and  $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ ,  $1 \leq i \leq n$ . Then there exist  $v_i \in \mathbb{F}_{q^2}$  such that  $u_i = v_i^2$ , for  $i = 1, \dots, n$ , and the generalized Reed-Solomon code  $GRS_{\frac{n}{2}}(\alpha, v)$  is an  $[n, \frac{n}{2}, \frac{n}{2} + 1]$  MDS Hermitian self-dual code over  $\mathbb{F}_{q^2}$ , where  $\alpha = (\alpha_1, \dots, \alpha_n)$  and  $v = (v_1, \dots, v_n)$ .

*Proof* Obviously,  $u_i (\neq 0) \in \mathbb{F}_q(\subseteq \mathbb{F}_{q^2})$  for  $1 \leq i \leq n$ . So there exist  $v_i (\neq 0) \in \mathbb{F}_{q^2}$  such that  $u_i = v_i^2$  for  $1 \leq i \leq n$ . The generalized Reed-Solomon code  $GRS_{\frac{n}{2}}(\alpha, v)$  is an  $[n, \frac{n}{2}, \frac{n}{2} + 1]$  MDS code over  $\mathbb{F}_{q^2}$ . For proving the generalized Reed-Solomon code  $GRS_{\frac{n}{2}}(\alpha, v)$  is Hermitian self-dual over  $\mathbb{F}_{q^2}$ , we only prove

$$(v_1 \alpha_1^l, \dots, v_n \alpha_n^l) \cdot (v_1^q \alpha_1^{kq}, \dots, v_n^q \alpha_n^{kq}) = 0, \quad 0 \leq l, k \leq \frac{n}{2} - 1.$$

From the choose of  $\alpha_i$ ,  $v_i$  and [8, Corollary 2.3],

$$(v_1 \alpha_1^l, \dots, v_n \alpha_n^l) \cdot (v_1^q \alpha_1^{kq}, \dots, v_n^q \alpha_n^{kq}) = (v_1 \alpha_1^l, \dots, v_n \alpha_n^l) \cdot (v_1 \alpha_1^k, \dots, v_n \alpha_n^k) = 0, \quad 0 \leq l, k \leq \frac{n}{2} - 1.$$

So the generalized Reed-Solomon code  $GRS_{\frac{n}{2}}(\alpha, v)$  is an  $[n, \frac{n}{2}, \frac{n}{2} + 1]$  MDS Hermitian self-dual code over  $\mathbb{F}_{q^2}$ .

Next we construct MDS Hermitian self-dual codes from constacyclic codes.

Let  $C$  be an  $[n, k]$   $\lambda$ -constacyclic code over  $\mathbb{F}_{q^2}$  and  $(n, q) = 1$ .  $C$  is considered as an ideal,  $\langle g(x) \rangle$ , of  $\frac{\mathbb{F}_{q^2}[x]}{x^n - \lambda}$ , where  $g(x) | (x^n - \lambda)$ . Simply,  $C = \langle g(x) \rangle$ .

**Lemma 4**<sup>[12]</sup> Let  $\lambda \in \mathbb{F}_{q^2}^*$ ,  $r = \text{ord}_{q^2}(\lambda)$ , and  $C$  be a  $\lambda$ -constacyclic code over  $\mathbb{F}_{q^2}$ . If  $C$  is Hermitian self-dual, then  $r|q+1$ .

**Lemma 5**<sup>[12]</sup> Let  $n = 2^a n'$  ( $a > 0$ ) and  $r = 2^b r'$  be integers such that  $2 \nmid n'$  and  $2 \nmid r'$ . Let  $q$  be an odd prime power such that  $(n, q) = 1$  and  $r|q+1$ , and let  $\lambda \in \mathbb{F}_{q^2}$  has order  $r$ . Then Hermitian self-dual  $\lambda$ -constacyclic codes over  $\mathbb{F}_{q^2}$  of length  $n$  exist if and only if  $b > 0$  and  $q \not\equiv -1 \pmod{2^{a+b}}$ .

Let  $r = \text{ord}_{q^2}(\lambda)$  and  $r|q+1$ .

$$O_{r,n} = \{1 + rj | j = 0, 1, \dots, n-1\}.$$

Then  $\alpha^i (i \in O_{r,n})$  are all solutions of  $x^n - \lambda = 0$  in some extension field of  $\mathbb{F}_{q^2}$ , where  $\text{ord} \alpha = rn$ .  $C$  is called a  $\lambda$ -constacyclic code with defining set  $T \subseteq O_{r,n}$ , if

$$C = \langle g(x) \rangle \quad \text{and} \quad g(\alpha^i) = 0, \quad \forall i \in T.$$

**Theorem 4** Let  $n = 2^a n' (a > 0)$  and  $r = 2^b r' (b > 0)$ .  $rn | q^2 - 1$ .  $\lambda \in \mathbb{F}_{q^2}^*$  with  $\text{ord} \lambda = r$ .  $q \not\equiv -1 \pmod{2^{a+b}}$ . If  $rn | 2(q+1)$ , there exists an MDS Hermitian self-dual code  $C$  over  $\mathbb{F}_{q^2}$  with length  $n$ ,  $C$  is a  $\lambda$ -constacyclic code with defining set

$$T = \left\{ 1 + rj \mid 0 \leq j \leq \frac{n}{2} - 1 \right\}.$$

*Proof* If  $rn | q^2 - 1$ ,  $C_{q^2}(i) = \{i\}$ , for  $i \in O_{r,n}$ , where  $C_{q^2}(i)$  denote the  $q^2$ -cyclotomic coset of  $i \pmod{rn}$ . And  $|T| = \frac{n}{2}$ ,  $C$  is an  $\left[n, \frac{n}{2}, \frac{n}{2} + 1\right]$  MDS  $\lambda$ -constacyclic code by the BCH bound of constacyclic code.

When  $rn | 2(q+1)$ ,  $q = \frac{rn}{2} - 1$ . Because  $q \not\equiv -1 \pmod{2^{a+b}}$ ,  $l$  is odd.

$$\begin{aligned} (-q)(1 + rj) &= -q - q r j \\ &\equiv 1 - \frac{rn}{2} + rj \\ &\equiv 1 + r\left(\frac{n}{2} + j\right) \pmod{rn}. \end{aligned}$$

So

$$(-q)T \cap T = \emptyset.$$

$C$  is MDS Hermitian self-dual by the relationship of roots of a constacyclic code and its Hermitian dual code's roots.

**Remark** The MDS Hermitian self-dual constacyclic code obtained from Theorem 4 is different with the MDS Hermitian self-dual constacyclic code in [12], because  $(q+1, q-1) = 2$  for an odd prime power  $q$ .

If  $r = 2$ ,  $C$  is negacyclic. Theorem 4 can be stated as follow.

**Corollary 2** Let  $n = 2^a n' (a \geq 1)$  and  $n'$  is odd. Let

$$q \equiv -1 \pmod{2^a n'} \text{ and } q \equiv 2^a - 1 \pmod{2^{a+1}},$$

where  $n' | n''$  and  $n''$  is odd. Then there exists an MDS Hermitian self-dual code  $C$  of length  $n$  which is negacyclic with defining set

$$T = \left\{ 1 + 2j \mid j = 0, 1, \dots, \frac{n}{2} - 1 \right\}.$$

Especially, when  $a = 1$ , Corollary 2 is similar as [5, Theorem 11].

From Theorem 3 and Theorem 4, we obtain the next theorem.

**Theorem 5** Let  $n \leq q+1$  and  $n$  be even. There exists an MDS Hermitian self-dual code with length  $n$  over  $\mathbb{F}_{q^2}$ .

## 4 MDS Hermitian Self-Dual Codes Obtained from Extended Cyclic Duadic Codes

Let  $D$  be an odd-like duadic code. Let  $\gamma \in \mathbb{F}_{q^2}$  be a solution to

$$1 + \gamma^{q+1}n = 0.$$

Obviously, the equation always has a solution in  $\mathbb{F}_{q^2}$ . Let  $c = (c_0, c_1, \dots, c_{n-1}) \in D$ . Define

$$\tilde{c} = (c_0, c_1, \dots, c_{n-1}, c_\infty), \quad \text{where } c_\infty = -\gamma \sum_{i=0}^{n-1} c_i.$$

Let  $\tilde{D} = \{\tilde{c} | c \in D\}$  be the extended code of  $D$ .

**Lemma 6**<sup>[2]</sup> Let  $D_1$  and  $D_2$  be a pair of odd-like duadic codes of length  $n$  over  $\mathbb{F}_{q^2}$ . If  $\mu_{-q}$  gives the splitting for  $D_1$  and  $D_2$ , then  $\tilde{D}_1$  and  $\tilde{D}_2$  are Hermitian self-dual.

**Lemma 7**<sup>[2]</sup> Let  $C$  be a cyclic code over  $\mathbb{F}_{q^2}$ . The extended code  $\tilde{C}$  is Hermitian self-dual if and only if  $C$  is an odd-like duadic code whose splitting is given by  $\mu_{-q}$ .

**Lemma 8**<sup>[2]</sup> Cyclic codes of length  $n$  over  $\mathbb{F}_{q^2}$  whose extended code is Hermitian self-dual exist if and only if for every prime  $r$  dividing  $n$ , either  $\text{ord}_r(q)$  is odd or  $\text{ord}_r(q^2)$  is even.

In [5], Guenda give the next theorem.

**Theorem 6**<sup>[5, Theorem 8]</sup> Let  $q = r^t$  be an odd prime power, and  $n = p^m \in \mathbb{F}_r$  a divisor of  $q^2 + 1$ , where  $p^m \equiv 1 \pmod{4}$ . Then there exists Hermitian self-dual codes over  $\mathbb{F}_{q^2}$  which are MDS and extended duadic codes with the splitting given by  $\mu_{-q}$  and with parameters  $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$ .

In the analysis of Theorem 6 in [5],  $D_1$  is an  $[n, \frac{n+1}{2}, \frac{n+1}{2}]$  MDS cyclic code with defining set

$$T = \left\{ \frac{n+3}{4}, \dots, \frac{3n-3}{4} \right\}.$$

And  $D_1$  is considered as an odd-like duadic code, when  $n = p^m (\equiv 1 \pmod{4})$ . Then the code

$$\tilde{D}_1 = \left\{ \tilde{c} = (c_0, c_1, \dots, c_{n-1}, c_\infty) | (c_0, c_1, \dots, c_{n-1}) \in D_1, c_\infty = -\gamma \sum_{i=0}^{n-1} c_i \right\},$$

where  $\gamma \in \mathbb{F}_{q^2}$  is a root of  $1 + \gamma^{q+1}n = 0$ , is an MDS Hermitian self-dual codes by Lemma 6.

Sometimes,  $n$  and  $q$  satisfy conditions of Theorem 6, but  $D_1$ , with defining set  $T$ , is not an odd-like duadic code. So it can be proved by Lemma 7 that  $\tilde{D}_1$  is not an (MDS) Hermitian self-dual codes.

**Example 1** Let  $p = 5$ ,  $n = 5^2$  and  $q = 7$ , then  $n$  and  $q$  satisfy conditions of Theorem 6.  $D_1$  is a  $[25, 13, 13]$  MDS cyclic code over  $\mathbb{F}_{7^2}$  with defining set

$$T = \{7, 8, \dots, 17, 18\}.$$



And  $12 \in (-7)T(\text{mod}25) \cap T$ .  $D_1$  is not an odd-like duadic code with defining set  $T$ . So it is proved by Lemma 7 that  $\tilde{D}_1$  is not an (MDS) Hermitian self-dual code over  $\mathbb{F}_{7^2}$ .

**Example 2** Let  $p = 5$ ,  $n = 5^2$  and  $q = 43$ , then  $n$  and  $q$  satisfy conditions of Theorem 6.  $D_1$  is a  $[25, 13, 13]$  MDS cyclic code over  $\mathbb{F}_{43^2}$  with defining set

$$T = \{7, 8, \dots, 17, 18\}.$$

And  $13 \in (-43)T(\text{mod}25) \cap T$ .  $D_1$  is not an odd-like duadic code with defining set  $T$ . So it is proved by Lemma 7 that  $\tilde{D}_1$  is not an (MDS) Hermitian self-dual code over  $\mathbb{F}_{43^2}$ .

Let  $n|q^2 + 1$ ,  $n \equiv 1 \pmod{4}$  and  $q$  be an odd prime power.  $D_1$  is an  $[n, \frac{n+1}{2}, \frac{n+1}{2}]$  MDS cyclic code over  $\mathbb{F}_{q^2}$  with defining set

$$T = \left\{ \frac{n+3}{4}, \dots, \frac{3n-3}{4} \right\}.$$

We want to prove that  $\tilde{D}_1$  is an MDS Hermitian self-dual code, so we must prove that  $D_1$  is an odd-like duadic code. It is equivalent to prove that

$$(-q)T(\text{mod}n) \cap T = qT(\text{mod}n) \cap T = \emptyset.$$

Note that  $-T(\text{mod}n) = T$ .

Let  $n = 4k + 1$ ,  $k \geq 1$ . So

$$T = \{k+1, \dots, 3k\}.$$

If  $qT(\text{mod}n) \cap T = \emptyset$  and  $qT(\text{mod}n) \cup T = \{1, 2, \dots, n-1\}$ , then

$$qT = \{1, \dots, k\} \cup \{3k+1, \dots, 4k\}.$$

There is an  $\alpha \in T$  such that  $q\alpha \equiv 1 \pmod{n}$ . And  $q^2 \equiv -1 \pmod{n}$ , so  $\alpha \equiv -q \pmod{n}$ .

We claim that

$$q \equiv \frac{n+3}{4} \text{ or } \frac{3n-3}{4} \pmod{n}.$$

If not, then

$$\frac{n+3}{4} < q \pmod{n} < \frac{3n-3}{4} \text{ and } \frac{n+3}{4} < -q \pmod{n} < \frac{3n-3}{4}.$$

Note that  $\frac{n+3}{4} \equiv -\frac{3n-3}{4} \pmod{n}$ . So

$$(q+1) \pmod{n} \in T, \quad (-q+1) \pmod{n} \in T.$$

$$q(-q+1) = -q^2 + q \equiv (1+q) \pmod{n} \in qT \cap T.$$

It is a contradiction to  $qT \cap T = \emptyset$ .

So

$$q \equiv \frac{n+3}{4} \text{ or } \frac{3n-3}{4} \pmod{n}.$$

And  $n|q^2 + 1$ .

$$q^2 + 1 \equiv \frac{n^2 + 6n + 9}{16} + 1 \text{ or } \frac{9n^2 - 18n + 9}{16} + 1 \equiv 0 \pmod{n}.$$

$$n \equiv 1 \pmod{4}, \quad (16, n) = 1.$$

So  $n|25$ .

$$n = 5 \text{ and } n = 25.$$

When  $n = 5$ ,

$$q \equiv 2 \pmod{5} \text{ or } q \equiv 3 \pmod{5}.$$

When  $n = 25$ ,

$$q \equiv 7 \pmod{25} \text{ or } q \equiv 18 \pmod{25}.$$

And  $n = 25$ ,  $q = 7 \equiv 7 \pmod{25}$  and  $q = 43 \equiv 18 \pmod{25}$  in Example 1 and Example 2. So when  $n = 25$ , it is impossible that there is an odd prime power  $q$ , with  $q \equiv 7 \pmod{25}$  or  $q \equiv 18 \pmod{25}$ , such that  $qT \cap T = \emptyset$ , where  $T = \{7, 8, \dots, 18\}$ .

When  $n = 5$  and  $n|q^2 + 1$ , it is easily to prove that Theorem 6 is correct, because  $T = \{\frac{n+3}{4}, \dots, \frac{3n-3}{4}\} = \{2, 3\}$ .

**Theorem 7** Let  $q = r^t$  be an odd prime power, and  $n = 5$  is a divisor of  $q^2 + 1$ . Then there exist Hermitian self-dual codes over  $\mathbb{F}_{q^2}$  which are MDS and extended duadic codes with the splitting given by  $\mu_{-q}$  and with parameters  $[6, 3, 4]$ .

If we want to obtain more extended cyclic duadic codes over  $\mathbb{F}_{q^2}$ , which are Hermitian self-dual, we shall require that  $n|q - 1$ ,  $(n, q + 1) = 1$  and  $2 \nmid n$  by the BCH bound of cyclic codes and Lemma 8. So we have the next theorem.

**Theorem 8** Let  $q = r^t$  be an odd prime power, and  $n|q - 1$ ,  $(n, q + 1) = 1$ . Then there exists Hermitian self-dual codes over  $\mathbb{F}_{q^2}$  which are MDS and extended duadic codes with the splitting given by  $\mu_{-q}$  and with parameters  $[n + 1, \frac{n+1}{2}, \frac{n+3}{2}]$ .

**Proof** As  $n|q - 1$  and  $(n, q + 1) = 1$ , there is a cyclic MDS  $[n, \frac{n+1}{2}, \frac{n+1}{2}]$  code  $D$  over  $\mathbb{F}_{q^2}$  with defining set  $T = \{1, 2, \dots, \frac{n-1}{2}\}$ . And

$$(-q)T \equiv (-1)T \equiv \{n - 1, n - 2, \dots, \frac{n+1}{2}\} \pmod{n}, \quad (-q)T \cap T = \emptyset.$$

So  $\tilde{D}$  is an MDS Hermitian self-dual code over  $\mathbb{F}_{q^2}$  with parameters  $[n + 1, \frac{n+1}{2}, \frac{n+3}{2}]$ . Theorem 8 is proved.

## 5 Conclusion

In this paper, we obtain many new MDS Euclidean self-dual codes by solving the equation (\*) in  $\mathbb{F}_q$ . We generalize the work of [8] to MDS Hermitian self-dual codes, and we construct new MDS Hermitian self-dual codes from constacyclic codes. We obtain that there exists an MDS Hermitian self-dual code with length  $n$  over  $\mathbb{F}_{q^2}$ , where  $n \leq q + 1$  and  $n$  is even. And we also discuss these MDS Hermitian self-dual codes, which are extended cyclic duadic codes. We give these corrections (Theorem 7 and Theorem 8) of Theorem 6 ([5, Theorem 8]).

## References

- [1] T. Aaron Gulliver, J. L. Kim. and Y. Lee, New MDS or near-MDS self-dual codes, IEEE Trans. on Inform. Theory, 4354-4360, 2008.
- [2] L. Dicuango, P. Moree and P. Solé, The lengths of Hermitian self-dual extended duadic codes, J. Pure Appl. Algebra, 223-237, 2007.
- [3] S. Georgiou and C. Koukouvinos, MDS self-dual codes over large prime fields, Finite Fields Appl., 455-470, 2002.
- [4] M. Grassel and T. Aaron Gulliver, On self-dual MDS codes, Proceedings of ISIT 2008, 1954-1957.
- [5] Kenza Guenda, New MDS self-dual codes over finite fields, Des. Codes Cryptogr. 31-42, 2012.
- [6] M. Harada and H. Kharaghani, Orthogonal designs and MDS self-dual codes, Austral. J. Combin., 57-67, 2008.
- [7] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, 2003.
- [8] L. F. Jin and C. P. Xing, New MDS self-dual codes from generalized Reed-Solomon codes, arXiv:1601.04467v1, 2016.
- [9] J. L. Kim and Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, J. Combin. Theory Ser. A, 105: 79-95, 2004.
- [10] C. D. Pang and C. B. Pang, Elementary Number Theory. (in Chinese) Beijing University Press, Beijing, 2002.
- [11] M. H. M. Smid, Duadic codes, IEEE. Trans. Inform. Theory. 432-433, 1983.

- [12] Y. S. Yang and W. C. Cai, On self-dual constacyclic codes over finite fields, Des. Codes Cryptogr., 74: 355-364, 2015.